Attorney Docket No. 16869P-097900US
Client Ref. No. 340300055US1

PATENT APPLICATION

POLICY SETTING SUPPORT TOOL

Inventors: **Masato ARAI**
Citizenship: Japan

Satoshi KAI
Citizenship: Japan

Assignee: Hitachi, Ltd.
6, Kanda Surugadai 4-chome
Chiyoda-ku, Tokyo, Japan
Incorporation: Japan

Entity: Large

TOWNSEND AND TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
(415) 576-0200

TITLE OF THE INVENTION

ポリシー設定支援ツール　(Policy Setting Support Tool)

BACKGROUND OF THE INVENTION

本発明は、コンピュータシステムが管理する情報資産に対するアクセスを、所定のポリシーに基づいてコントロールするアクセス制御システムに用いるポリシー設定支援ツールに関する。

一般のコンピュータシステムでは、マルチユーザマルチタスクＯＳが備えるユーザ認証機構と、該認証結果に基づいたアクセス制御機構を用いて情報その他コンピュータ資源の保護を実現しているケースが多い。具体的には、上記ＯＳが実装された情報処理装置を利用する際に、ユーザは必ず自己のユーザＩＤとパスワードを入力し、認証を受ける。

上記情報処理装置が管理する全てのファイル各々には、ファイル読み出しや書き込み等のアクセスタイプ毎に、ユーザＩＤとグループＩＤを用いてアクセス可能なユーザを定義したアクセスコントロールリスト（ポリシーと称す）がセキュリティ属性情報として割り当てられている。

ユーザがアプリケーションプログラムを介してファイルへアクセスした場合、上記ＯＳは、アクセス要求元となるユーザのＩＤ及び該ユーザが所属するグループのＩＤを、アクセス対象となるファイルやディレクトリに割り当てられたポリシーと照合し、当該リストに上記ユーザが含まれている場合に限りアクセスを許可するといった制御を行う。

また、アクセス要求元の情報として、上記ユーザＩＤやグループＩＤだけでなく、例えばアクセス手段となるプログラムの識別子まで確認すれば、より厳密なアクセス制御が可能となる。

このようなアクセス制御の方法は、例えば Japanese Laid Open Patent Publication No. 2001-337864（文献１）に開示されている。ただし、不正アクセスを防止するには、本来の利用目的であるサービス提供や業務遂行の上で必要最小限のアクセスのみ許可されるよう、上記ポリシーを設定しておくことが重要である。

その他、Japanese Laid Open Patent Publication No. 2002-108818（文献２）には、セキュリティポリシーの作成に要する時間を短縮するために、複数の雛形のポリシーから自己に見合ったものを選択し、修正しながらポリシーを作成する方法が開示されている。

先に述べたように、情報資産を安全に利用するためには、当該情報への必要最小限のアクセスのみ許可するようにポリシーを定義することが重要である。しかし、ユーザＩＤやグループＩＤだけでなく、アクセス手段となるプログラムの識別子まで組み合わせてポリシーを定義することは、厳密なアクセス権チェックができる代わりに、そのポリシー作成に手間がかかる。例えば、どのようなデータにアクセスするかといったソフトウェアの仕様を知らなければ、適切なポリシーは設定できない。

ソフトウェアが複数のプログラムから構成されている場合は、特に難しいと言える。上記文献２に記載されている方法を用いても、雛形のポリシーを自己に見合ったものに修正するのは全て利用者自身であるため、ソフトウェアの仕様を知らなければ、どこをどのように修正すべきか判断できないケースも発生し得る。

また、プログラムアップデートによるプログラムファイル自体の変更が発生したり、ユーザやグループの登録内容に変更が発生したり、更には情報資産であるファイルやディレクトリが、削除・移動・名称書き換え等により変更されることで、現在のポリシーの記述と一致しなくなれば、適切なアクセス制御ができなくなるという問題もある。

SUMMARY OF THE INVENTION

本発明は、利用するソフトウェアの仕様を知らなくても、コンピュータの利用目的を果たす上で適切なファイルアクセスのみを許可するようにポリシーを設定可能な、ポリシー設定支援ツールを提供する。

本発明は、アクセス主体となるユーザやプログラムの情報の他、アクセス対象となるファイルやディレクトリ等に変更があった場合でも、簡易な操作により関連するポリシーの設定内容を更新可能な、ポリシー設定支援ツールを提供する。

本発明は、コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、上記ポリシー情報の作成に要する作業負荷を軽減するためのポリシー設定支援ツールであって、当該ポリシー設定支援ツールは、アクセス主体となるサブジェクトの種類毎に用意した情報と、アクセス対象となるオブジェクトの種類毎に用意した情報から、適切なポリシーを作成するものであり、上記サブジェクトの種類毎に用意した情報とは、サブジェクトの種類毎に標準的あるいは推奨のポリシーを記述したサンプル情報と、サブジェクトの正常な動作を記録したアクセスログ情報と、対象のコンピュータシステムにインストールされているサブジェクトのインストール先パス名を含むインストール情報とからなり、上記オブジェクトの種類毎に用意した情報とは、オブジェクトの種類毎にアクセス手段として利用される頻度の高いサブジェクトの情報を記述した関連付け情報からなり、更に上記ポリシー設定支援ツールは、上記サブジェクトの動作を監視して上記アクセスログ情報に記録するためのアクセス監視部と、上記サンプル情報と上記インストール情報とを照合して差分を検出する差分検出部と、上記サンプル情報と上記関連付け情報と上記差分検出部による検出結果とからポリシーの原案を作成するポリシー生成部と、ポリシーの原案を表示して利用者による更なるポリシーの修正および保存をするためのユーザインタフェース部とから構成されることを特徴としている。

上記ポリシー設定支援ツールによれば、例えばソフトウェアの種類毎にサンプルとなるポリシーが提供され、且つ対象のコンピュータシステムに適合したポリシーの原案まで自動的に作成できるので、利用者はソフトウェアの仕様を知らなくても、適切なポリシーが容易に設定可能となる。

また、本発明は、上記ポリシー設定支援ツールにおいて、当該ポリシー設定支援ツールの利用者は、上記ユーザインタフェース部を通じて、上記サンプル情報と、上記関連付け情報と、上記アクセスログ情報とから、１つ以上の情報を用いてポリシーの原案を作成し、当該ポリシー原案を元に必要に応じて更に修正を加え、修正後のポリシーを保存することで、上記ポリシー情報を設定することを特徴としている。

これにより、上記サンプルとなるポリシーが用意されていない場合でも、上記関連付け情報やアクセスログ情報からポリシーの原案が作成できるので、利用者はソフトウェアの仕様を知らなくても、適切なポリシーが容易に設定可能となる。

また、本発明は、コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、上記ポリシー情報の維持に要する作業負荷を軽減するためのポリシー設定支援ツールであって、アクセス対象となるオブジェクトならびにアクセス主体となるサブジェクトに関する最新情報と、当該最新情報と設定済みのポリシーの内容とを照合しながら更新すべき項目を検出するための差分検出部と、当該差分検出部による検出結果の表示処理と、利用者による目視確認および上記ポリシーの更新処理をするためのユーザインタフェース部とから構成されることを特徴としている。

これにより、アクセス主体となるサブジェクトの情報や、アクセス対象となるオブジェクトに変更があった場合でも、更新すべき項目を自動的に検出して表示できるので、簡易な操作で関連するポリシーの更新が可能となる。

また、本発明は、上記ポリシー設定支援ツールにおいて、上記差分検出部による検出処理は、定期的に、あるいは利用者からの要求を受けた時点で実行されるものであり、差分を検出した場合には、当該差分情報を、上記ユーザインタフェース部を通じて利用者向けに表示し、上記ポリシー設定支援ツールの利用者は、上記ユーザインタフェース部を通じて表示される上記差分情報を目視で確認し、当該表示通りに更新すべきかどうかを判断し、更新すべきであれば上記ユーザインタフェース部を通じて必要な修正を加えた上で、上記ポリシー情報を保存することを特徴としている。

これにより、利用者は上記ユーザインタフェース部を通じて、差分情報の確認と、ポリシーの修正および保存まで、ポリシーの更新に必要な処理を全て行うことができる。

また、定期的な差分検出処理も可能とすることで、利用者が自ら上記差分検出部に対して要求を出さなくても差分情報を取得できるようになるため、無効なポリシー記述を放置することなく、常に適切なポリシーに基づくアクセス制御が可能となる。

また、本発明は、コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、上記ポリシー情報の作成に要する作業負荷を軽減するためのポリシー設定支援ツールであって、上記コンピュータシステムは、アクセス対象となるオブジェクトの種類毎にアクセス手段として利用される頻度の高いサ

ブジェクトの情報を記述した関連付け情報を備えており、上記ポリシー設定支援ツールは、上記関連付け情報からポリシー情報を作成することを特徴としている。

このようにオブジェクトの種類毎にアクセス可能なサブジェクトを決定することで、ポリシー情報の設定が容易になるだけでなく、各オブジェクトの移動やコピー、削除が発生しても、同一種類のオブジェクトである限り同一のポリシー情報に基づくアクセス制御が可能となり、ポリシー情報の変更が不要となる。

また、本発明は、上記ポリシー設定支援ツールにおいて、オブジェクトへのアクセス手段を用途別に指定するための用途別サブジェクト指定手段を備えており、当該用途別サブジェクト指定手段を利用して指定されたプログラムであれば、複数種類のオブジェクトに関連付けられたサブジェクトとして上記ポリシー情報を作成することを特徴としている。

これにより、関連付け情報のみを用いた場合よりも、柔軟なポリシー情報が設定可能になるとともに、上記ポリシー設定支援ツールと同様に、各オブジェクトの移動やコピー、削除が発生しても、同一種類のオブジェクトである限りポリシー情報の変更は不要となる。

また、本発明のポリシー設定支援ツールは、上記ポリシー情報に違反するアクセスが発生した場合に上記アクセス制御機構から通知を受けて、当該アクセスの対象となるオブジェクトを管理するコンピュータシステムの利用者に対してメッセージを伝え、上記利用者による判断に基づいて所定の処理を実行する手段を備えており、上記利用者による判断とは、上記ポリシー違反のアクセスを以後全て許可するか、今回のアクセスのみ許可するか、禁止するかのいずれかであり、上記ポリシー違反のアクセスを以後全て許可する場合には、上記ポリシー設定支援ツールによる所定の処理として上記アクセスが正当なアクセスとなるようポリシー情報を変更し、上記アクセス制御機構に対しては上記アクセスが正当であることを通知し、上記ポリシー違反のアクセスを今回のみ許可する場合には、所定の処理として上記ポリシー情報は変更せずに、上記アクセス制御機構に対しては上記アクセスが正当であることを通知し、上記ポリシー違反のアクセスを禁止する場合には、所定の処理として上記ポリシー情報は変更せず、上記アクセス制御機構に対しては上記アクセスが不正であることを通知することを特徴としている。

更に、上記ポリシー設定支援ツールは、上記ポリシー情報に登録されていない新種のオブジェクトに対して、当該オブジェクトに関連付けられたサブジェクトからアクセスが発生した時に、上記アクセス制御機構から通知を受け、上記コンピュータシステムの利用者に対してメッセージを伝え、上記利用者による判断に基づいて所定の処理を実行する手段を備えており、上記利用者による判断とは、新種のオブジェクトに対する当該オブジェク

トに関連付けられたサブジェクトからのアクセスを許可するか、禁止するかのいずれかであり、上記アクセスを許可する場合には、上記ポリシー設定支援ツールによる所定の処理として上記アクセスが正当なアクセスとなるようポリシー情報を変更して、上記アクセス制御機構に対しては上記アクセスが正当であることを通知し、上記アクセスを禁止する場合には、上記ポリシー情報は変更せず、上記アクセス制御機構に対しては上記アクセスが不正であることを通知することを特徴としている。

また更に、上記ポリシー設定支援ツールは、上記ポリシー情報に登録された情報とは一部異なるサブジェクトからアクセスが発生した時に、上記アクセス制御機構から通知を受け、上記コンピュータシステムの利用者に対してメッセージを伝え、上記利用者による判断に基づいて所定の処理を実行する手段を備えており、上記利用者による判断とは、上記サブジェクトからのアクセスを許可するか、禁止するかのいずれかであり、上記アクセスを許可する場合には、上記ポリシー設定支援ツールによる所定の処理として上記サブジェクトが正当なものとなるようポリシー情報を変更して、上記アクセス制御機構に対しては上記アクセスが正当であることを通知し、上記アクセスを禁止する場合には、上記ポリシー情報を変更せず、上記アクセス制御機構に対しては上記アクセスが不正であることを通知することを特徴としている。

上記の特徴により、コンピュータシステムの正当な利用を妨げることなく、簡単な操作によりポリシー情報を修正可能となる。

本発明によれば、ポリシーの作成および維持に要する作業負荷を軽減することが可能になる。

These and other benefits are described throughout the present specification. A further understanding of the nature and advantages of the invention may be realized by reference to the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

図１は、本実施形態におけるポリシー設定支援ツールの一構成例を示す。

図２は、ポリシー設定支援ツールを利用するためのコンピュータシステムの一構成例を示す。

図３は、インストール情報と関連付け情報とサンプル情報とアクセスログの一例を示す。

図４は、本実施形態において、ポリシー設定画面４００の一例を示す。

図５は、本実施形態において、ポリシー情報１２０の一例を示す。

図６は、本実施形態において、簡易設定インタフェース６００の一例を示す。

図７は、サンプル情報１０７からポリシーを作成する処理のフローチャートを示す。

図８は、関連付け情報１０６からポリシーを作成する処理のフローチャートを示す。

図９は、アクセスログ１０８からポリシーを作成する処理のフローチャートを示す。

図１０は、差分検出部１０４によるポリシー更新処理のフローチャートを示す。

図１１は、編集用ボックス４２０に表示するポリシーの変更情報の一例を示す。

図１２は、第二の実施形態におけるポリシー設定支援ツールの一構成例を示す。

図１３は、第二の実施形態におけるポリシーファイル１２２０の一例を示す。

図１４は、第二の実勢形態におけるポリシー作成処理のフローチャートを示す。

図１５は、第二の実勢形態におけるポリシー参照・編集画面の一例を示す。

図１６は、アクセス制御部との連携によるポリシー情報変更のフローチャートを示す。

図１７は、変更後のプログラムからアクセスが発生した時に表示するメッセージの一例を示す。

図１８は、未登録のプログラムからアクセスが発生した時に表示するメッセージの一例を示す。

図１９は、新種のファイルに対してアクセスが発生した時に表示するメッセージの一例を示す。

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

以下、図を用いて第一の実施形態を説明する。

図１は、本実施形態のポリシー設定支援ツールの一構成例である。ポリシー設定支援ツール１００は、ユーザインタフェース部１０１と、ポリシー生成部１０２、アクセス監視部１０３、差分検出部１０４、インストール情報１０５、関連付け情報１０６、サンプル情報１０７、アクセスログ１０８から構成される。

１１０はアクセス制御部であり、サブジェクト１１１からオブジェクト１１２へのアクセスの可否をポリシー情報１２０の記述内容に従って判定し、ポリシーに合致したアクセスのみ許可し、ポリシー違反のアクセスであれば上記サブジェクト１１１にエラーを返すといった処理を行う。

このようなアクセス制御は、一般的なオペレーティングシステム（ＯＳ）でも標準で備えているが、それらが参照するポリシー情報の多くは、オブジェクトへアクセス可能なサブジェクトを、ユーザやグループの識別子を用いて指定したものである。

これに対して、本実施形態のポリシー設定支援ツールが扱うポリシー情報とは、ユーザやグループの識別子だけでなく、少なくともアクセスする際に用いるプログラムの情報を組み合わせてアクセス権を指定したものである。

なお、サブジェクト情報１１３は、本実施例においてはインストールされているプログラムファイル群や、登録されているユーザ・グループに関する情報を指す。

上記ポリシー設定支援ツール１００は、上記各種情報１０５～１０７や、上記サブジェクト１１１からオブジェクト１１２へのアクセスを記録したアクセスログ１０８を利用しながらポリシー情報１２０の設定作業を容易にするものである。また、上記サブジェクト情報１１３を参照しながら、ポリシーの更新作業を容易にするものでもある。

図２は、上記ポリシー設定支援ツール１００を利用するために必要なシステムの一例を示したものである。図２において、情報処理装置２００は、中央演算処理装置ＣＰＵ２０１ａと、主記憶２０２ａ、外部記憶装置２０３ａ、入力装置２０４、表示部２０５、ＬＡＮなどのネットワーク２２０とのやりとりを制御する通信コントローラ２０６ａが、バスなどの通信線（バスという）２０７ａに接続することで形成されている。

図１にて示したオブジェクト１１２や、サブジェクト情報１１３、ポリシー情報１２０

は、上記外部記憶装置２０３ａに格納され、必要に応じて主記憶２０２ａの領域に読み出して利用される。

また、上記サブジェクト１１１やアクセス制御部１１０は、主記憶２０２ａにロードされ、実行可能プログラムとして上記ＣＰＵ２０１ａによって処理されるものである。特にアクセス制御部１１０は、オペレーティングシステム（ＯＳ）の一部、あるいはＯＳに組み込み可能なプログラムとして処理される。

同様に、上記ポリシー設定支援ツール１００も、主記憶２０２ａにロードされ、上記ＣＰＵ２０１ａによって処理されるものである。

また、ポリシー設定支援ツール１００のうち、ユーザインタフェース部１０１は、上記表示部２０５にユーザインタフェースを表示し、入力装置２０４を介して入力されるデータやコマンドに応じて各種処理を実行する。

また、インストール情報１０５や、関連付け情報１０６、サンプル情報１０７、アクセスログ１０８については、外部記憶装置２０３ａに格納しておき、必要に応じて主記憶２０２ａの領域に読み出して利用してもよい。

ここまでは、情報処理装置２００にて利用されるポリシー情報１２０を、上記ポリシー設定支援ツール１００により設定および更新するために必要なシステム構成である。

次に、例えば入力装置２０４や表示部２０５をもたないサーバ２１０におけるポリシー設定および更新処理を、上記情報処理装置２００から行うためのシステム構成について説明する。

サーバ２１０ａは、ＣＰＵ２０１ｂ、主記憶２０２ｂ、外部記憶装置２０３ｂの他に、通信コントローラ２０６ｂをバス２０７ｂに接続することで形成される。通信コントローラ２０６ｂは、主記憶２０２ｂにロードされて実行中のプログラムが、ネットワーク２２０を介して他のネットワークノードとデータを交換するために利用する装置である。

上記アクセス制御部１１０が、サーバ２１０ａのＯＳあるいはＯＳに組み込み可能なプログラムとして主記憶２０２ｂにロードされてＣＰＵ２０１ｂにより処理され、同じく主記憶２０２ｂにロードされてＣＰＵ２０１ｂにより処理されるプログラムをサブジェクト１１１とみなし、当該サブジェクトからオブジェクト１１２へのアクセスを制御することを前提とし、以下説明する。

なお、ポリシー情報１２０やオブジェクト１１２、サブジェクト情報１１３は、外部記憶装置２０３ｂに格納してもよいし、他のネットワークノードと共有可能な外部記憶装置を別途用意して格納してもよい。

このようなシステム構成において、本実施形態のポリシー設定支援ツール１００を利用する場合は、少なくとも入力装置２０４と表示部２０５の利用を前提とする上記ユーザインタフェース部１０１を、情報処理装置２００側の主記憶２０２ａにて実行させ、それ以外のポリシー生成部１０２、アクセス監視部１０３、差分検出部１０４はサーバ２１０側の主記憶２０２ｂにて実行させ、互いにネットワーク２２０を介してデータ交換を行いながら各種処理を実行する。

また、インストール情報１０５や、関連付け情報１０６、サンプル情報１０７、アクセスログ１０８については、外部記憶装置２０３ｂに格納してもよいし、他のネットワークノードと共有可能な外部記憶装置を別途用意して格納してもよい。

これにより、遠隔地にある複数のサーバ２１０ｂから２１０ｘに対しても、同一の情報処理装置からポリシーの設定および更新が可能となる。

図５は、上記ポリシー情報１２０の一例を示したものである。上述のように、本実施形態のポリシー設定支援ツール１００が扱うポリシー情報とは、オブジェクトへアクセス可能なサブジェクトを、プログラム名とユーザ・グループの識別子との組み合わせで指定したものである。

図５の例で言うと、ユーザ名”www”の権限で実行しているプログラム”/as/wserv.exe”のみ、オブジェクト名”/www/pub/*”で示されるファイル群に対してアクセス”R”（読み出し）を許可するといったものである。図５における特徴値とは、プログラムの特徴を表す数値のことであり、例えばプログラムファイルのサイズや、ハッシュ関数を用いて算出した値を利用する。

アクセス発生時に、上記アクセス制御部１１０が特徴値を確認することで、不当に改ざんされたプログラムによるアクセスからオブジェクトを保護することも可能となる。また、図５における時間とは、アクセスを許可する時間帯のことであり、特に指定がない場合は、終日アクセス可能となるよう”00:00－24:00”と設定する。

また、図５におけるソフトウェア名称とは、上記プログラムが構成するソフトウェアに

付けられた名称である。これは、利用者がポリシーを編集する際に、ソフトウェア名称を用いてプログラムを指定可能とすることを目的に登録されたものであり、上記アクセス制御部１１０によるアクセス権チェックの際には無視される情報である。

図３は、上記インストール情報１０５や、関連付け情報１０６、サンプル情報１０７、アクセスログ１０８の一例を示したものである。インストール情報１０５とは、上記サブジェクト情報に格納されているプログラムに関する情報を、ソフトウェアの種類毎に分類して管理するためのものである。

その内容は、ソフトウェア名称と、実行ファイル名称、当該実行ファイルのインストール先となるディレクトリ名、更には当該ソフトウェアをアンインストールする際に実行すべきアンインストールプログラムの名称といった情報からなる。

図３の例では、”Ｍ３メール 3.0”というソフトウェア名称がインストールされており、その実体となる実行ファイルが”M3MAIL.exe”であり、当該実行ファイルのインストール先が”/m3/”ディレクトリの下であり、アンインストールプログラムの名称が”/m3/uninstall.exe”であることを表している。

このような情報は、一般的なオペレーティングシステム（ＯＳ）でも管理している場合が多いことから、本実施形態のポリシー設定支援ツール１００が独自に管理せずに、ＯＳが管理しているインストール情報を利用することも考えられる。

次に、関連付け情報１０６とは、オブジェクト１１２をアクセスする際に、そのアクセスに利用される頻度の高いプログラムの情報を、オブジェクトの種類毎に管理するためのものである。図３の例では、ファイル名の拡張子が”txt”のオブジェクトへアクセスする際には、利用者からの特別な指示がない限り、実行ファイル名称が”/tools/gpad.exe”のプログラムを利用することを意味している。

このような情報も、一般的なＯＳが管理している場合が多いことから、本実施形態のポリシー設定支援ツール１００が独自に管理せずに、ＯＳが管理している関連付け情報を利用することも考えられる。

３つ目に、サンプル情報１０７とは、ソフトウェアの種類毎に標準的な、あるいは推奨のポリシー情報を記述したものである。図３の例では、ソフトウェア名称が”アタッチサーバ2.0”というプログラムを利用するならば、オブジェクト名が”/www/pub/*”で表されるファイルに対しては、実行ファイル名称が”/as/wserv.exe”のプログラムが、ユーザ・

グループ名が”www”の権限で実行している場合に限り、アクセスタイプ”R”つまり読み出しのみ許可することを表している。

４つ目に、アクセスログ１０８とは、上記サブジェクト１１１からオブジェクト１１２へのアクセスを、上記アクセス監視部１０３により監視して、当該アクセス内容を記録したものである。図３に示したアクセスログの一行目の例では、オブジェクト名に示されるファイル”/datafile.db”に対して、サブジェクト情報として示されているプログラム名”/db/hdbr.exe”のプログラムがユーザ名”system”の権限によって、アクセスタイプに示されるアクセス”RW”（読み出しと書き込み）を実行したことを表している。

図４は、ポリシー設定支援ツール１００のユーザインタフェース部１０１が、当該ツールの利用者向けに提供するポリシー設定画面４００の一例を示すものである。利用者は、図２の表示部２０５に表示された上記ポリシー設定画面４００を利用することにより、ポリシー情報１２０の設定や更新、参照といった各種編集作業が可能となる。

ポリシー設定画面４００のうち、４１０ａはポリシー情報１２０に現在登録されているポリシー一覧を表示するボックスである。当該ポリシー表示ボックス４１０ａは、アクセス対象となるオブジェクト名と、アクセス主体となるサブジェクト情報と、許可されたアクセスタイプと、アクセス可能な時間帯を表す情報から構成される。

図４（ａ）の例では、サブジェクト情報として、ソフトウェアの名称を表示している。これは、図３で示したインストール情報１０５に格納されているソフトウェア名称と同じものである。これにより、利用者にとってポリシーの大要を把握し易くなるという効果が期待できる。

４１１ａは、ポリシーの表示を切り替えるための切替ボタンであり、利用者が当該切替ボタン４１１ａを押下すると、図４（ｂ）の４１０ｂに示すように、サブジェクト情報の表示が、プログラム名とプログラムファイルの特徴値、およびユーザ・グループ名といった、より詳細なものへと切り替わる。反対に、図４（ｂ）の切替ボタン４１１ｂを押下すると、図４（ａ）の４１０ａのような、ソフトウェア名称だけの表示へと切り替わる。

このようなサブジェクト情報の表示切り替えを可能とするためには、上記図３に示したインストール情報１０５に格納されたソフトウェア名称を、図５に示すようにポリシー情報１２０に対しても識別子として登録し、各プログラムとソフトウェア名称の対応関係を保持しておけばよい。

または、上記ソフトウェア名称の代わりに、ユニークな識別番号を各ソフトウェアに対して割り当てて、上記インストール情報１０５と上記ポリシー情報１２０の両方に登録してもよい。

また、複数のプログラムファイルから構成されるソフトウェアであれば、それらプログラムファイルには全て同一の識別番号あるいは識別子を、上記ポリシー情報１２０に登録する。多くの場合、それらプログラムファイルの格納先は共通のディレクトリ下であることから、共通のディレクトリ下にあるプログラムファイルに対して同一のソフトウェア識別番号あるいは識別子を割り当てればよい。

上記ユーザインタフェース部１０１は、上記切替ボタン４１１が押下される度に、ポリシー情報１２０を参照しながら上記ポリシー表示ボックス４１０内のサブジェクト情報の表示内容を切り替えることになる。

４２０は、ポリシーを生成、変更するための編集用ボックスである。４２１は、編集用ボックス４２０に記述したポリシーを上記ポリシー表示ボックス４１０に追加して、ポリシー情報１２０に保存するための追加ボタンである。

上記編集用ボックス４２０には、オブジェクト名とサブジェクト情報、アクセスタイプ、時間を指定できるが、これら項目を利用者が一つ一つ入力してもよいし、後述するように簡易設定ボタン４３０を利用して指定することもできる。

また、上記ポリシー表示ボックス４１０からポリシーを選択すると、上記ユーザインタフェース部１０１が、当該ポリシーを上記編集用ボックス４２０に表示するので、既に登録済みのポリシーを一部変更する際には、上記ポリシー表示ボックス４１０に表示されたポリシーから変更したいものを選択して上記編集用ボックス４２０に表示し、必要な修正を加えてから上記追加ボタン４２１を押下すればよい。

上記ポリシー設定画面４００には、上記簡易設定ボタン４３０の他、サンプル登録ボタン４３１、更新ボタン４３２、削除ボタン４３３、終了ボタン４３４がある。以下、これらボタンの意味について説明する。

簡易設定ボタン４３０は、上記サンプル情報１０７や、関連付け情報１０６、アクセスログ１０８等を利用して、ポリシー原案を自動生成する際に押下するボタンである。当該処理については後述する。

サンプル登録ボタン４３１は、上記編集用ボックス４２０の表示内容を上記サンプル情報１０７に登録し、以後サンプルポリシーとして再利用可能なものとする際に押下するボタンである。

更新ボタン４３２は、上記ポリシー情報１２０に登録されているポリシーを、最新のオブジェクトやサブジェクト情報１１３に合わせて更新する際に押下するボタンである。この処理についても後述する。

登録済みのポリシーを一部削除したい場合には、上記ポリシー表示ボックス４１０に表示されたポリシーから削除したいものを選択して、削除ボタン４３３を押下する。また、ポリシー編集作業を終了する場合には、終了ボタン４３４を押下する。

図６は、上記簡易設定ボタン４３０を押下したときに、図２の表示部２０５に出現する簡易設定インタフェースの一例を示したものである。利用者は、簡易設定インタフェース６００を通じて、上記サンプル情報１０７を利用したポリシー原案作成や、上記関連付け情報１０６を利用したポリシー原案作成、更には上記アクセスログ１０８を利用したポリシー原案作成を実行することができる。

図６の６０１は、インストールされているソフトウェア一覧表示ボックスであり、上記ユーザインタフェース部１０１が、上記インストール情報１０５およびサンプル情報１０７を参照して、現在インストールされていて且つサンプルポリシーが用意されているソフトウェアのみを表示する。

利用者が、これらソフトウェアのサンプルポリシーを利用してポリシーの原案を作成する場合には、各ソフトウェアに対応したチェックボックス６０３ａにチェックを付けて、原案作成ボタン６０８を押下すればよい。

図６の６０２は、特定のソフトウェアとの関連付けがされているファイル拡張子一覧表示ボックスであり、上記ユーザインタフェース部１０１が上記関連付け情報１０６を参照して表示する。当該関連付け情報を利用してポリシーの原案を作成する場合には、各拡張子に対応したチェックボックス６０３ｂにチェックを付けて、原案作成ボタン６０８を押下すればよい。

図６の６０５は、監視したいプログラムを指定するための入力ボックスであり、ここにプログラムファイル名を入力して開始ボタン６０６を押下すると、上記アクセス監視部によるアクセス監視と上記アクセスログ１０８への記録を開始する。終了ボタンを押下する

と、上記アクセス監視とアクセスログ記録を終了する。

その後で、上記原案作成ボタン６０８を押下すると、アクセスログ１０８を利用してポリシー原案を作成することができる。なお、上記プログラムの指定は、プログラムファイル名の代わりに、ソフトウェアの名称で指定できるものでもよい。

上記のように作成されたポリシー原案は、上記ユーザインタフェース部１０１の処理により、図４の編集用ボックス４２０に表示される。当該ポリシー原案をベースに、利用者が一部修正を加えるなど、編集作業を行ってから上記追加ボタン４２１を押下すると、当該編集されたポリシーを上記ポリシー表示ボックス４１０に追加すると共に、ポリシー情報１２０にも保存する。

図６の６０９は、キャンセルボタンであり、上記簡易設定インタフェース６００の処理を終了して、図４のポリシー設定画面４００へ戻る際に押下する。

図７は、サンプル情報１０７からポリシー原案を生成する処理手順の一例を示したものである。ステップ７０１は、上記ユーザインタフェース部１０１へのコマンド入力であり、これは図６のソフトウェア一覧表示ボックス６０１からソフトウェアを選択して、上記原案作成ボタン６０８を押下することに相当する。

ステップ７０２では、上記ポリシー生成部１０２により、上記選択されたソフトウェアに対応するサンプル情報を取得する。ステップ７０３では、上記差分検出部１０３により、上記サブジェクト情報１１３やオブジェクト１１２を参照して、上記サンプル情報との差分データを作成する。

これは、ソフトウェアのインストール先や、ディレクトリ構成が標準と異なる場合、上記サンプル情報がそのまま利用できないことがあるためである。ステップ７０４では、上記ポリシー生成部１０２により、上記サンプル情報と差分データを基に、対象となる情報処理装置やサーバに相応しいポリシーの原案を生成する。

このとき、アクセス許可されるプログラムの特徴値算出も併せて行う。また、アクセス許可する時間帯については、特に指定がない限り、終日（00:00－24:00）に設定しておく。ステップ７０５では、上記ユーザインタフェース部１０１により、上記ポリシーの原案を、上記図４の編集用ボックス４２０に表示する。

ステップ７０６では、表示されたポリシー原案に対して、利用者自身により必要な修正

を加える。この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ７０７では、上記修正後のポリシーを、上記ポリシー情報１２０へ保存する。このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名の他、ソフトウェア名称も付加して保存する。

次に図８を用いて、関連付け情報１０６を利用したポリシー生成の処理手順の一例を説明する。ステップ８０１は、上記ユーザインタフェース部１０１へのコマンド入力であり、これは図６のファイル拡張子一覧表示ボックス６０２から拡張子を選択して、上記原案作成ボタン６０８を押下することに相当する。

ステップ８０２では、上記関連付け情報１０６を参照して、上記利用者が選択した拡張子に関連付けられたプログラムの実行ファイル名称を取得する。ステップ８０３では、上記ポリシー生成部１０２により、上記取得した情報を基にポリシーの原案を生成する。

このとき生成されるポリシーの原案は、オブジェクト名と、プログラム名と、プログラムの特徴値と、時間帯のみ指定されており、ユーザ・グループ名やアクセスタイプは指定していない。ただし、図２に示した上記情報処理装置２００やサーバ２１０が利用しているＯＳ自身が、上記アクセス制御部１１０とは異なる独自のアクセス制御機構を備えている場合はその通りでない。

つまり、当該ＯＳ独自のアクセス制御機構があれば、各オブジェクトへのアクセス条件として、ユーザ・グループの情報や、アクセスタイプが設定されているはずである。そこで、例えば上記ポリシー生成部１０２がこれらユーザ・グループの識別子やアクセスタイプを取得して、上記ポリシーの原案に取り込むものであってもよい。

また、同じ拡張子をもつファイルでも、これらユーザ・グループやアクセスタイプが異なるものは、オブジェクト名を区別してそれぞれ個別のポリシーとなるよう原案を作成する。

このようにして生成したポリシー原案は、ステップ８０４にて上記ユーザインタフェース部１０１が、上記図４の編集用ボックス４２０に表示する。ステップ８０５では、表示されたポリシー原案に対して、利用者自身により必要な修正を加える。

この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ８０６では、上記修正後のポリシーを、上記ポリシー情報１２０へ保存する。

このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名の他、ソフトウェア名称も付加して保存する。当該ソフトウェア名称は、上記インストール情報１０５より取得する。

次に図９を用いて、上記アクセスログ１０８を利用したポリシー生成処理手順の一例を説明する。ステップ９０１は、上記ユーザインタフェース部１０１へのコマンド入力であり、これは図６の入力ボックス６０５にプログラムを指定して、上記開始ボタン６０６を押下することに相当する。

ステップ９０２では、上記アクセス監視部１０３により、上記指定されたプログラムから発行されるファイルアクセスを監視して、その内容を上記アクセスログ１０８に記録する。この処理は、上記図６の終了ボタン６０７を押下するまで継続する。

ステップ９０３では、上記ポリシー生成部１０２により、上記アクセスログ１０８からポリシー原案を生成する。このとき、上記アクセスログ１０８に記録されたアクセスは、正当なアクセスとして許可されるようにポリシー原案を作成する。

また、サブジェクトとなるプログラムの特徴値も算出し、上記ポリシー原案に取り入れる。時間帯指定については、特に指定がない限り”00:00－24:00”（終日）とする。

このようにして生成したポリシー原案は、ステップ９０４にて上記ユーザインタフェース部１０１が、上記図４の編集用ボックス４２０に表示する。ステップ９０５では、表示されたポリシー原案に対して、利用者自身により必要な修正を加える。

この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ９０６では、上記修正後のポリシーを、上記ポリシー情報１２０へ保存する。

このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名の他、ソフトウェア名称も付加して保存する。当該ソフトウェア名称は、上記インストール情報１０５より取得する。

以上の図７から図９の処理を、利用者が必要に応じて繰り返したり、組み合わせたりしながらポリシーを作成することになる。

次に、図１０を用いて上記差分検出部１０４の処理手順について説明する。これは、上記オブジェクト１１２やサブジェクト情報１１３に変更が生じた場合にも、登録済みのポリシー情報１２０への反映を容易にするための処理である。

ステップ１００１は、例えば上記ユーザインタフェース部１０１へのコマンド入力であり、これは上記図４の更新ボタン４３２を押下することに相当する。あるいは、図２の上記情報処理装置２００やサーバ２１０に搭載されたＯＳが備えるスケジューラ機能等により、差分検出部１０４の処理を定期的に実行させるものであってもよい。

そして差分が検出された場合には、ポリシーの記述を見直す必要があることを、上記ユーザインタフェース部１０１を通じて利用者に通知することで、無効なポリシーの記述を放置することなく、常に適切なポリシーに基づくアクセス制御が可能となる。

ステップ１００２では、差分検出部１０４が上記ポリシー情報１２０を参照し、当該ポリシー情報１２０に登録されているオブジェクト名とサブジェクト情報を取得する。ステップ１００３では、オブジェクトとサブジェクトに関する最新情報を、上記オブジェクト１１２とサブジェクト情報１１３とから取得し、上記ポリシー情報１２０の内容と照合する。

ステップ１００４では、上記照合処理の結果、更新の必要があると思われるポリシーについてはその内容を上記ユーザインタフェース部１０１に渡し、図１１に示すように、上記編集用ボックス４２０に表示する。このとき、変更のあった部分が他よりも目立つよう強調表示する。

利用者は、当該変更内容を目視で確認し（ステップ１００５）、更新しても問題ないと判断するならば、必要な修正を加えた上で、図１１の更新ボタン４２２を押下することで、正式に上記ポリシー情報１２０の内容を更新できる（ステップ１００６）。仮に、プログラムのアップデートをした覚えがないのに、プログラムの特徴値に変更があった場合は、プログラムファイルの不当な改ざんが発生した可能性もあると考えられ、この場合は、利用者はポリシーの更新をせずに上記プログラムファイル改ざんの原因を確認すればよい。

以上述べたように、本実施形態によれば、ソフトウェアの仕様を詳しく知らなくても、ソフトウェアの種類毎に用意したサンプルポリシーや、関連づけ情報、ソフトウェアのアクセスログを利用することで、適切なポリシーを短時間に作成することができる。

また、オブジェクトやサブジェクトの情報に変更があった場合でも、変更すべきポリシ

一の部分が利用者にとって容易に判るよう表示でき、且つ簡易な操作で更新可能であることから、常に適切なポリシー情報に基づくアクセス制御が可能となる。

次に、第二の実施形態を説明する。

図１２は、第二の実施形態となるポリシー設定支援ツールの一構成例である。ポリシー設定支援ツール１２００は、ユーザインタフェース部１２０１と、ポリシー生成部１２０２、差分検出部１２０４から構成され、インストール情報１０５や、関連付け情報１０６、オブジェクト共有情報１０９、サブジェクト情報１１３を参照しながらポリシーを生成し、ポリシーファイル１２２０に登録する役割をもつ。なお、サブジェクト情報１１３は、本実施例においてはインストールされているプログラムファイル群を指す。

１１０はアクセス制御部であり、サブジェクト１１１からオブジェクト１１２へのアクセスの可否をポリシーファイル１２２０の記述内容に従って判定し、ポリシーに合致したアクセスのみ許可し、ポリシー違反のアクセスであれば上記ポリシー設定支援ツール１２００を通じてユーザ１２１０に通知し、その応答を受けて上記サブジェクト１１１にエラーを返す、あるいはアクセスを許可するといった処理を行う。

１２４０は認証処理部であり、ユーザ情報１２３０に登録されている情報を参照しながらユーザ１２１０の識別と認証の処理を行う。ユーザ１２１０は、上記オブジェクト１１２を利用するのに先立って、上記認証処理部１２４０による識別認証を受ける必要がある。このとき、ユーザ１２１０は例えば自己のユーザＩＤとパスワードを入力することになり、ユーザ情報１２３０と一致すれば、以後サブジェクト１１１を実行してオブジェクト１１２へのアクセスを発行できるようになる。なお、上記サブジェクト１１１は、例えば実行中のプログラムであり、且つ当該プログラムを実行したユーザのＩＤを継承しており、上記アクセス制御部１１０が許可する範囲でオブジェクト１１２へアクセス可能となる。

このような認証処理部とアクセス制御部は、一般的なオペレーティングシステム（ＯＳ）でも標準で備えているが、それらが参照するポリシー情報の多くは、オブジェクトへアクセス可能なサブジェクトを、ユーザやグループの識別子を用いて指定したものである。

これに対して、第二の実施形態のポリシー設定支援ツールが扱うポリシー情報とは、オブジェクトの種類毎にアクセス可能なプログラムを指定したものである。

つまり第二の実施形態におけるアクセス制御部１１０は、例えば一般的なＯＳが備えるアクセス制御機能と、上記ポリシー設定支援ツールが扱うポリシー情報を用いたアクセス

制御機能とを併せ持つものと言える。このうち、一般的なＯＳが備えるアクセス制御機能では、図１３の１３００に示すようなポリシー情報を参照する。これは、ファイル名と、その所有者名と、アクセス権から構成され、全てのファイルやディレクトリに対して必ず何らかのアクセス権が設定されている。アクセス権は更に３種類のユーザに対するアクセス権を指定でき、左から順に、　所有者のアクセス権、　所有者と同じグループに属するユーザのアクセス権、　所有者とは異なるグループに属するユーザのアクセス権、となっている。図中のＲＷＤＸはアクセスのタイプを表し、それぞれ読み出し（Ｒ）、書き込み（Ｗ）、削除（Ｄ）、実行またはチェンジディレクトリ（Ｘ）を意味する。通常、このようなポリシー情報１３００は、ＯＳが標準で備えるツール等を用いて設定できる。

一方、図１３の１３１０は、ポリシー設定支援ツール１２００によって設定するポリシー情報であり、ファイルの種類と、プログラム名と、プログラムの特徴値から構成される。上記ポリシー情報１３００に示すように、従来のアクセス権はファイルやディレクトリ毎に指定するものであったが、ポリシー情報１３１０ではアクセスに用いるプログラムをファイルの種類毎に設定することが特徴である。これは、一般的にファイルの種類が異なれば利用するプログラムも異なるという点に着目し、プログラムを指定する場合には個々のファイルやディレクトリ単位でなく、ファイルの種類毎に指定することが有効であるとの考えに基づく。ファイルの種類はファイル名の拡張子によって区別でき、例えばＨＴＭＬファイルであれば“＊．ｈｔｍｌ”のように記述すれば、拡張子ｈｔｍｌをもつ全てのファイルを指定したことになる。また、全種類のファイルを指定する場合には、“＊．＊”と記述すればよい。なお、上記特徴値とはプログラムの特徴を表す数値のことであり、例えばプログラムファイルのサイズや、ハッシュ関数を用いて算出した値を利用する。

ここで、ポリシー情報１３００を例にとると、ファイル“/users/satou/memo.txt”は、ユーザ satou によってＲＷＤが可能となるが、ポリシー情報１３１０によれば、拡張子が“ｔｘｔ”のファイルに対しては、いかなるユーザであっても“/tools/gpad.exe”のプログラム、あるいは全てのファイル（＊．＊）にアクセス可能なプログラムを利用する必要がある。また別の言い方をすれば、全てのファイルにアクセス可能なプログラムとしてポリシー情報１３１０に登録されたプログラムを用いてファイル“/users/satou/memo.txt”にアクセスしても、ポリシー情報１３００の方で上記ファイルにアクセス権を与えられたユーザでなければ、上記アクセス制御部１１０によりアクセスは禁止される。これにより、ポリシー情報１３００のみを利用していた従来のアクセス制御と比べ、ポリシー情報１３１０を併せて利用することで不正なプログラムによるアクセスを防止でき、厳重なオブジェクト管理を実現できる。

このようなポリシー情報１３１０を簡易な操作で設定可能とするポリシー設定支援ツー

ル１２００を利用するために必要なシステムは、上記第一の実施形態と同様に、図２の情報処理装置２００が一例として挙げられる。

図２において、情報処理装置２００は、中央演算処理装置ＣＰＵ２０１ａと、主記憶２０２ａ、外部記憶装置２０３ａ、入力装置２０４、表示部２０５、通信コントローラ２０６ａが、バスなどの通信線(バスという)２０７ａに接続することで形成されている。

図１２にて示したオブジェクト１１２や、サブジェクト情報１１３、インストール情報１０５、関連付け情報１０６、オブジェクト共有情報１０９、ポリシーファイル１２２０、ユーザ情報１２３０は、上記外部記憶装置２０３ａに格納され、必要に応じて主記憶２０２ａの領域に読み出して利用される。このうち、サブジェクト情報１１３と、インストール情報１０５、関連付け情報１０６の内容は、第一の実施形態の説明に用いたものと同じである。

また、上記サブジェクト１１１やアクセス制御部１１０、認証処理部１２４０は、主記憶２０２ａにロードされ、実行可能プログラムとして上記ＣＰＵ２０１ａによって処理されるものである。特にアクセス制御部１１０と認証処理部１２４０はＯＳの一部、あるいはＯＳに組み込み可能なプログラムとして処理される。

同様に、上記ポリシー設定支援ツール１２００も、主記憶２０２ａにロードされ、上記ＣＰＵ２０１ａによって処理されるものである。

また、ポリシー設定支援ツール１２００のうち、ユーザインタフェース部１２０１は、上記表示部２０５にユーザインタフェースを表示し、入力装置２０４を介して入力されるデータやコマンドに応じて各種処理を実行する。

図１４は、上記ポリシー設定支援ツール１２００によるポリシー情報の作成処理フローを示したものである。当該作成処理は、例えばポリシー設定支援ツール１２００を上記情報処理装置２００へインストールした時や、ユーザ１２１０が上記ツール１２００を起動した時に自動的に開始するものであってもよい。または、上記ツール１２００が定期的に実行するものでもよい。更には、後述する図１５に示すポリシー参照・編集画面１５００にある更新ボタン１５０８をユーザ１２１０が押下した時でもよい。

ステップ１４０１では、差分検出部１２０４が、関連付け情報１０６に登録されているファイルの種類と、上記ポリシー情報１３１０に登録されているファイルの種類を比較して、その差分を検出する。このうち、ポリシー情報１３１０に登録されていて、且つ関連

付け情報１０６に登録されていないファイルの種類があれば、ポリシー情報１３１０から当該ファイルの種類に関する記述を削除する。一方、ポリシー情報１３１０に未登録のファイルの種類があれば、ステップ１４０２で各ファイルの種類毎に関連付けられたプログラム（実行ファイル）の名称を、関連付け情報１０６から取得する。このとき、図１９に示すようなメッセージボックス１９００を表示部２０５に表示してユーザ１２１０に確認してもよい。ここで、ユーザがボタン１９０１「はい」を押下すればステップ１４０３の処理へ移り、ボタン１９０３「いいえ」を押下すれば差分検出処理（ステップ１４０１）に戻る。あるいは、関連付けられたプログラムであれば、逐一ユーザに確認することなくステップ１４０３の処理へ移るといった実施形態も考えられる。

ステップ１４０３では、サブジェクト情報１１３から上記実行ファイルの特徴値を算出してポリシー情報１３１０を生成する。また、既にポリシー情報１３１０に登録されている実行ファイルのうち、特徴値が変更されているものがあれば、上記差分検出部１２０４からユーザインタフェース部１２０１へその旨通知し、ステップ１４０４にて図１７に示すようなメッセージボックス１７００を表示部２０５に表示してユーザ１２１０に確認する。上記メッセージボックス１７００において、ユーザがボタン１７０１「はい」を押下すれば、変更後のプログラムは正当なプログラムであるとして上記ポリシー情報１３１０を更新する。また、ボタン１７０２「いいえ」を押下すれば、上記ポリシー情報１３１０は更新しない。

ステップ１４０５では、上記ユーザインタフェース部１２０１が、上記処理により生成したポリシー情報１３１０を、図１５のポリシー参照・編集画面１５００の形式で表示部２０５に表示する。上記関連付け情報１０６から生成したポリシーは、図１５の中の「ファイルの種類とプログラムの対応一覧」１５０１に含まれている。

当該一覧１５０１には、ＯＳを構成する各種プログラム（システムプログラムと呼ぶ）と関連付けられたファイルの種類と、上記ＯＳ上で動作するアプリケーションプログラムと関連付けられたファイルの種類とが混在することになる。両者を区別して表示するために、ポリシー設定支援ツール１２００は、先ずアプリケーションプログラムの名称を上記インストール情報１０５から取得し、次にそれらアプリケーションプログラムと関連付けられたファイルの種類を上記関連付け情報１０６より取得する。そして、それ以外のもの、つまり上記システムプログラムと関連付けられたファイルの種類とは、色分けして上記一覧１５０１に表示する。

このように表示された上記一覧１５０１の設定内容を上記ポリシーファイル１２２０に格納するためには、保存ボタン１５０９を押下する。このとき、ポリシー情報１３１０か

ら除外したい関連付けがあれば、そのチェックボックス１５０５のマーク（レ印）を外してから保存ボタン１５０９を押下すればよい。ただし、除外されたファイルの種類に対しては、どのプログラムを用いてアクセスしてもよいことになる。

ここで、上記関連付け情報１０６から作成したポリシー情報１３１０のもとでは、別のプログラムとの間でオブジェクトを共有する機能をもつプログラムが正常に動作しなくなる場合がある。たとえば、表計算の機能がないワープロソフトが、その文書中に、表計算ソフトで作ったグラフを貼り込めるうえ、グラフに変更を加えたい場合は、ワープロ文書中のグラフをダブルクリックすることにより表計算ソフトが自動的に起動する、といった機能を持つ場合である。表計算ソフトで作成したグラフは、もともと表計算ソフトと関連付けられた種類のファイルに格納されているため、上記ワープロソフトから上記グラフを貼り込むときに、関連付けられていないファイルへのアクセスが発生する。当該アクセスは、上記関連付け情報１０６から作成したポリシー情報１３１０により、不正なアクセスとして扱われることになる。

これらアクセスを許可するのであれば、上記ポリシー設定支援ツール１２００が、（1）オブジェクトの共有機能をもつプログラムの名称（2）上記プログラムから貼り込み可能なオブジェクトの種類（3）上記オブジェクトの格納元となるファイルの種類の順に情報を取得し、（1）のプログラムから（3）のファイルの種類へのアクセスを許可するポリシーを生成して上記ポリシー情報１３１０に追加すればよい。このとき、上記プログラムの特徴値についても、上記サブジェクト情報１１３から算出して登録する。上記（1）から（3）までの情報をあわせて、ここではオブジェクト共有情報１０９とする。当該オブジェクト共有情報１０９は、ＯＳがコンピュータに関するあらゆる設定情報を集中管理するためのデータベースに含まれており、そこには上記関連付け情報１０６やインストール情報１０５も格納されている。

図１５で言えば、プログラム間でオブジェクトの共有を許可するためのチェックボックス１５０２にマーク（レ印）をつけて保存ボタン１５０９を押下すると、上記ポリシー設定支援ツール１２００が上記データベースの情報をもとに、自動的にポリシー情報１３１０を作成して保存する。更に、詳細設定ボタン１５０３を押下すると上記オブジェクト共有情報を詳細設定画面１５２０に表示し、プログラム毎に貼り込み可能なオブジェクトの種類、つまりアクセス可能なファイルの種類をきめ細かく設定できるようにしても良い。

当該詳細設定画面１５２０では、オブジェクトの共有機能をもつプログラムをプルダウンメニュー１５２１から選択し、当該プログラムから貼り込み可能なオブジェクトを、オブジェクトとファイルの種類の一覧表示ボックス１５２２にて選択指定（マーク付与）す

ればよい。実際には、初期設定時に上記チェックボックス１５０２にマークを付ければ、上記ボックス１５２２では貼り込み可能なオブジェクト全てにチェックマークが付いた状態となるようにし、そこから不要なものがあればマークを消していくことにする。例えば、オブジェクト「３Ｄ図面」が標準で格納されているファイル「＊．ｆｉｇ」に対して、プログラム「/ap/wordproc.exe」からアクセスすることが業務上不要であれば、詳細設定画面１５２０にて、上記オブジェクト「３Ｄ図面」のマークを消せばよい。以上のやり方で設定したポリシーは、保存ボタン１５０９を押下することでポリシー情報１３１０に反映される。

次に、ポリシー参照・編集画面１５００におけるプログラム指定ボックス１５０４は、例えば業務遂行上、各種ファイルへアクセスする際に用いるプログラムを指定するためのボックスである。これらも、関連付け情報１０６から作成したポリシーだけでは正常に動作しないと思われるプログラムであり、例えば各ファイルのコピーや移動、削除といったファイル操作用のプログラムや、コンピュータウィルスを検出して駆除するためのウィルス対策ソフト、障害時に重要なファイルを復旧するためのバックアップツール、ファイルの圧縮・解凍ツールなどがある。その他、電子メールやWWWにより各種ファイルを送受信するケースも考えられる。プログラム指定ボックス１５０４では、ユーザにとって分かり易くなるように、これらプログラムを用途別に指定可能とする。

ポリシー情報１３１０の初期設定時は、いずれのプログラムも指定されていない状態となるが、ＯＳが標準で備えているプログラムがある場合は、ポリシー設定支援ツール１２００が上記インストール情報１０５からそれらプログラムのソフトウェア名称を取得して、上記プログラム指定ボックス１５０４に表示してもよい。これにより、ユーザ１２１０によるプログラム選択作業を軽減できる。ＯＳが標準で備えるプログラムとは異なるものを指定する場合には、ユーザ１２１０または上記情報処理装置２００の管理者が参照ボタン１５０６を押下すると、上記インストール情報１０５からソフトウェア名称の一覧が表示され、その一覧から任意のプログラムを選択指定できる。インストール情報１０５に登録されていないソフトウェアであれば、プログラムファイル名を直接指定してもよい。また、電子メールやブラウザによるファイル送受信は、情報セキュリティを考えれば控えたほうが望ましいので、別の実施形態として、これらのプログラムは上記プログラム指定ボックス１５０４から選択指定できなくしてもよい。

上記のようにプログラムを選択してから保存ボタン１５０９を押下すると、上記ポリシー生成部１２０２はサブジェクト情報１１３から該当するプログラムファイルを検索してその特徴値を算出するとともに、そのプログラムが全種類のファイル（＊．＊）に対してアクセス可能となるようポリシー情報１３１０を作成し、上記ポリシーファイル１２２０

に保存する。その他の方法として、上記プログラムによってアクセス可能な対象は全種類のファイルでなく、例えばアプリケーションプログラムと関連付けられた種類のファイルに対してアクセス可能となるようポリシー情報１３１０を作成するものであってもよい。もしくは、アクセス可能な対象を更に細かく指定するために、ファイルの種類の一覧表示から選択指定させるものであってもよい。用途別に指定されたプログラムに対しては、その用途についても併せてポリシー情報１３１０に登録しておくことで、以後のポリシー情報設定時に、現在の設定内容をプログラム指定ボックス１５０４に表示することが可能となる。

また、ファイルのネットワーク共有を許可するためのチェックボックス１５０７を有効にして保存ボタン１５０９を押下すると、各種ファイルがネットワークで共有可能となるようポリシー情報１３１０を作成して保存する。このときアクセス権を与えるべきプログラムは、ＯＳが標準で備えているファイル共有用のサーバプログラムであるが、通常のアプリケーションプログラムとは異なり上記インストール情報１０５には登録されていない場合があるため、本実施例のように上記プログラム指定ボックス１５０４とは区別して扱ってもよい。

更新ボタン１５０８は、上記ポリシー作成処理フロー（ステップ１４０１から１４０５）の処理を繰り返してポリシー情報１３１０を更新するときに押下するボタンである。また、閉じるボタン１５１０を押下すれば、ユーザインタフェース部１２０１の処理を終了してポリシー参照・編集画面１５００を表示部２０５から消す。

次に、上記アクセス制御部１１０とポリシー設定支援ツール１２００の連携によりポリシー情報１３１０を適宜変更していく方法を、図１６を用いて説明する。

ステップ１６０１では、上記サブジェクト１１１からオブジェクト１１２へのアクセスをアクセス制御部１１０により検知し、ステップ１６０２にて上記アクセスをポリシーファイル１２２０の記述内容と照合する。このとき、一般的なＯＳが備えるアクセス制御ではポリシー情報１３００との照合によりアクセス権を判定するが、本実施の形態においてはポリシー情報１３１０との照合も併せて実施し、いずれのポリシーにも合致したアクセスであれば「適合」とみなしてステップ１６０９にて当該アクセスを許可する。

上記アクセスがポリシー情報１３００と合致しない場合、上記アクセス制御部１１０はアクセス要求元となるサブジェクト（プログラム）へ直ちにエラーを返して上記アクセスを禁止するが、ポリシー情報１３１０と合致しない場合には、ポリシー設定支援ツール１２００の処理に移り、ステップ１６０３以降の処理を実行する。ステップ１６０３では、

アクセス制御部１１０からの通知内容に基づいてメッセージを表示部２０５に表示する。このとき表示するメッセージには３種類あり、サブジェクト（プログラム）の特徴値が一致しない場合には図１７を、サブジェクト（プログラム）の名称が一致しない場合には図１８を、オブジェクト情報（ファイルの種類）がポリシーに登録されていない場合には図１９をそれぞれ表示する。

図１７のメッセージボックス１７００では、アクセス要求元となるプログラムの特徴値がポリシー情報１３１０の記述と一致しない場合に、プログラムが変更されている可能性があることをユーザ１２１０に伝えるものである。ステップ１６０４では、ユーザ１２１０は「はい」ボタン１７０１か、「いいえ」ボタン１７０２のいずれか一つを選んで押下することになる。「はい」ボタン１７０１を押下すると、ステップ１６０５にてポリシー設定支援ツール１２００はポリシー情報１３１０を変更（特徴値を変更）し、上記アクセス制御部１１０に上記アクセスが「適合」であることを通知する。「いいえ」ボタン１７０２を押下すると、正当なプログラムではないとみなして、ステップ１６０７にてポリシー情報１３１０は変更せず、上記アクセス制御部１１０に上記アクセスが「違反」であることを通知する。その他の実施形態として、ユーザ１２１０による判断だけでなく、例えば図２に示したネットワーク２２０を介して、上記変更されたプログラムが正当なものかどうかを、当該プログラムを製造または販売しているサイトへ問い合わせるためのボタンを、上記メッセージボックス１７００に追加することも考えられる。この場合、各プログラム毎にその製造または販売元となるサイトの情報（アドレス）を、上記インストール情報１０５やポリシー情報１３１０にて保持しておき、ユーザが上記問い合わせ用のボタンを押下したときに該当するサイトへ自動的に問い合わせるなどの処理が必要となる。

図１８のメッセージボックス１８００は、ある種類（例えば拡張子がｄｏｃ）のファイルに対してアクセス権をもたないプログラムからアクセス要求があった場合に、不正なプログラム、あるいは未登録のプログラムからのアクセスであることをユーザ１２１０に伝えるものである。ステップ１６０４では、ユーザ１２１０は「はい」ボタン１８０１か、「今回のみ」ボタン１８０２か、「いいえ」ボタン１８０３のいずれか一つを選んで押下することになる。「はい」ボタン１８０１を押下すると、以後上記プログラムから上記種類（拡張子がｄｏｃ）のファイルへのアクセスを許可するよう、ステップ１６０５にてポリシー情報１３１０を変更し、上記アクセス制御部１１０に上記アクセスが「適合」であることを通知する。「今回のみ」ボタン１８０２を押下すると、ステップ１６０６にてポリシー情報１３１０は変更せずに上記アクセスが「適合」であることを通知する。これにより、今回のアクセスは許可されるが、次回同じアクセスが発生した場合は再度メッセージボックス１８００が表示されることになる。また、「いいえ」ボタン１８０３を押下すると、不正なアクセスとみなして、ステップ１６０７ではポリシー情報１３１０は変更せず、上記アク

セスが「違反」であることを通知する。

図１９のメッセージボックス１９００は、ポリシー情報１３１０に登録されていない種類のファイルに対してアクセス要求があった場合に、ポリシー設定支援ツール１２００が上記関連付け情報１０６から上記種類のファイルに関する関連付け情報を取得し、ユーザ１２１０に伝えるものである。ただし上記メッセージボックス１９００は、上記種類のファイルと関連付けられたプログラムからのアクセス要求であった場合に表示するものであり、関連付けられたプログラム以外からのアクセス要求であった場合の処理は、上記メッセージボックス１８００で説明した通りである。メッセージボックス１９００では、ユーザ１２１０は「はい」ボタン１９０１か、「いいえ」ボタン１９０３のいずれか一つを選んで押下することになる。「はい」ボタン１９０１を押下すると、ステップ１６０５にてポリシー設定支援ツール１２００は上記関連付けられたプログラムからのアクセスが以後許可されるようにポリシー情報１３１０を変更し、上記アクセス制御部１１０に上記アクセスが「適合」であることを通知する。「いいえ」ボタン１９０３を押下すると、上記関連付け情報は妥当でないとみなして、ステップ１６０７にてポリシー情報１３１０は変更せず、上記アクセス制御部１１０に上記アクセスが「違反」であることを通知する。

以上述べた第二の実施の形態で、情報セキュリティの観点から見た有効な使い方を述べる。例えば電子メールやブラウザなどの通信機能をもつプログラムは、不正なプログラムの持ち込みや機密情報流出といったセキュリティホールとなる恐れがあるので、全種類のファイルにアクセス可能なプログラムとして指定しないことが望ましい。ポリシー設定支援ツール１２００が関連付け情報１０６から生成したポリシー情報１３１０であれば、電子メールやブラウザから利用できるファイルの種類は限定される。もし、業務の中で電子メールやブラウザを用いて文書ファイルを送受信する必要があった場合には、当該文書ファイルへのアクセス時に上記メッセージボックス１８００が表示されるので、そこで「今回のみ」ボタン１８０２を選べばよい。これにより業務には支障なく、且つ不正なプログラムによるファイル送受信を防止することが可能となる。

上記ポリシーファイル１２２０、特にポリシー情報１３１０が不当に書き換えられないようにするためには、例えばポリシーファイル１２２０へアクセス可能なプログラムを、ポリシー設定支援ツール１２００に限定するよう、予めポリシー情報１３１０に記述しておくことが有効である。

また、企業などの組織で運用する場合には、ポリシー情報１３１０は組織で決定するものであり、ユーザ１２１０によってポリシー情報１３１０を任意に変更されるのは好ましくないケースもある。つまり、上記ポリシー設定支援ツール１２００は組織で決めたポリ

シーを設定する際に管理者が利用するものであり、それ以外の状況で管理者以外の人物が利用するものではない。この場合は、上記ポリシーファイル１２２０へアクセス可能なプログラムの限定に加えて、ポリシーファイル１２２０には例えばＯＳの管理者だけがアクセス可能となるよう、予めポリシー情報１３００に記述しておくことが有効である。ただし、ＯＳ管理者の認証情報（例えばパスワード）が一般ユーザに悪用されないよう、厳重に管理しておく必要はある。

更に、管理者以外のユーザ１２１０に対しては、上記アクセス制御部１１０によるメッセージボックス１７００～１９００の表示処理は提供せず、ポリシー情報１３１０に違反するアクセスが発生したときには無条件にエラーを返すものとする。これは、図１６のステップ１６０２で違反と判定した場合に、ステップ１６１０の処理へジャンプすることに相当する。このような管理者向けと一般ユーザ向けの処理の切り替えは、環境設定情報として上記ポリシーファイル１２２０の一部に格納しておき、上記アクセス制御部１１０がその環境設定情報を参照し、管理者向けであれば図１６のステップ１６０３から１６０８の処理を追加し、その他一般ユーザ向けであればポリシー情報１３１０に違反するアクセスは全てエラーを返すようにすればよい。

また、多数の情報処理装置にて共通のポリシー情報を利用するならば、上記ポリシー設定支援ツールにより作成したポリシー情報を、各情報処理装置に配布して利用することで運用管理上の負荷を軽減することも可能である。特に、第二の実施形態にて示したポリシー情報１３１０は、ファイルのパス名でなく種類毎にポリシーを記述したものであるため、ファイルの移動やコピー、削除等が発生してもファイルの種類が変わらない限り同一のポリシー情報１３１０にて保護可能となる。したがって、各情報処理装置で共通のポリシー情報１３１０を利用すれば、同じセキュリティ効果が期待できる。

各情報処理装置で共通のポリシー情報１３１０を作成する方法としては、上記第二の実施形態で述べたように、設定対象となる情報処理装置にインストールされたポリシー設定支援ツール１２００を用いてもよいが、更に運用管理上の負荷を軽減するために、ネットワーク２２０を介して接続されているリモートのサーバまたは情報処理装置から設定する方法も考えられる。この場合、例えば設定対象となる情報処理装置にて図示していない代理プログラムを実行し、ネットワーク２２０を介してリモートのサーバまたは情報処理装置にて実行するポリシー設定支援ツール１２００と通信可能な状態をつくり、上記代理プログラムからは設定対象の情報処理装置にある関連付け情報１０６、インストール情報１０５、オブジェクト共有情報１０９を読み出してポリシー設定支援ツール１２００へ送信し、ポリシー設定支援ツール１２００からは作成したポリシー情報１３１０を上記代理プログラムに返信してポリシーファイル１２２０に格納すればよい。

なお、上記各実施形態において、情報処理装置とサーバにて実行される各プログラムは、予め各装置の記憶装置に格納されていてもよいし、図示していない着脱可能な記憶媒体または通信媒体（すなわちネットワークまたはネットワークを伝搬する搬送波）を介して、上記記憶部に導入されてもよい。

The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense. It will, however, be evident that various modifications and changes may be made thereto without departing from the spirit and scope of the invention as set forth in the claims.

WE CLAIM

請求項１

コンピュータが管理する資産をポリシー情報に基づいてアクセス制御するアクセス制御部を備えたコンピュータシステムにおいて、前記ポリシー情報を作成するためのポリシー設定支援ツールであって、

前記サブジェクトの種類毎に用意した情報とは、サブジェクトの種類毎に標準的あるいは推奨のポリシーを記述したサンプル情報と、サブジェクトの正常な動作を記録したアクセスログ情報と、対象のコンピュータシステムにインストールされているサブジェクトのインストール先パス名を含むインストール情報とからなり、

前記オブジェクトの種類毎に用意した情報とは、オブジェクトの種類毎にアクセス手段として利用される頻度の高いサブジェクトの情報を記述した関連付け情報からなり、

前記ポリシー設定支援ツールは、

前記サブジェクトの動作を監視して前記アクセスログ情報に記録するためのアクセス監視部と、

前記サンプル情報と前記インストール情報とを照合して差分を検出する差分検出部と、

前記サンプル情報と前記関連付け情報と前記差分検出部による検出結果とからポリシーの原案を作成するポリシー生成部と、

ポリシーの原案を表示して利用者による更なるポリシーの修正および保存をするためのユーザインタフェース部とから構成される。

請求項２

請求項１記載のポリシー設定支援ツールであって、

前記ユーザインタフェース部を通じて、ユーザの操作に従い、前記サンプル情報と、前記関連付け情報と、前記アクセスログ情報とから、１つ以上の情報を用いてポリシーの原案を作成する手段と、

当該ポリシー原案への修正操作を受け付け、修正後のポリシーを保存することで、前記ポリシー情報を設定する手段を備える。

請求項３

コンピュータが管理する資産をポリシー情報に基づいてアクセス制御するアクセス制御部を備えたコンピュータシステムにおいて、前記ポリシー情報を維持するためのポリシー設定支援ツールであって、

アクセス対象となるオブジェクトならびにアクセス主体となるサブジェクトに関する最新情報と、当該最新情報と設定済みのポリシーの内容とを照合しながら更新すべき項目を検出するための差分検出部と、

当該差分検出部による検出結果からポリシーの原案を作成するポリシー生成部と、

ポリシーの原案を表示して利用者による目視確認および前記ポリシーの更新処理をするためのユーザインタフェース部とから構成される。

請求項４

請求項３記載のポリシー設定支援ツールであって、

前記差分検出部による検出処理は、定期的に、あるいは利用者からの要求を受けた時点で実行されるものであり、差分を検出した場合には、当該差分情報を、前記ユーザインタフェース部を通じて利用者向けに表示し、

前記ポリシー設定支援ツールの利用者は、前記ユーザインタフェース部を通じて表示される前記差分情報を目視で確認し、当該表示通りに更新すべきかどうかを判断し、更新すべきであれば前記ユーザインタフェース部を通じて必要な修正を加えた上で、前記ポリシー情報を保存することを特徴とする。

請求項５

コンピュータが管理する資産をポリシー情報に基づいてアクセス制御するアクセス制御部を備えたコンピュータシステムにおいて、前記ポリシー情報を作成するためのポリシー設定支援ツールであって、

アクセス対象となるオブジェクトの種類毎にアクセス手段として利用される頻度の高いサブジェクトの情報を記述した関連付け情報を備え、

当該関連付け情報からポリシー情報を作成する手段を備える。

請求項６

請求項５記載のポリシー設定支援ツールであって、

前記ポリシー設定支援ツールは、オブジェクトへのアクセス手段を用途別に指定するための用途別サブジェクト指定手段を備えており、

当該用途別サブジェクト指定手段を利用して指定されたプログラムを、複数種類のオブジェクトにアクセス可能なサブジェクトとして前記ポリシー情報を作成する手段を備える。

請求項７

請求項５記載のポリシー設定支援ツールであって、

前記コンピュータシステムは、複数のサブジェクト間でオブジェクトを共有するためのオブジェクト共有処理部を備えたサブジェクトの識別子一覧と、当該サブジェクトから利用可能なオブジェクトの種類とを記述したオブジェクト共有情報を備えており、

前記ポリシー設定支援ツールは、前記オブジェクト共有情報に登録されたサブジェクトに対して、当該サブジェクトから利用可能なオブジェクトへのアクセスを全て許可、または一部許可するポリシー情報を作成する手段を備える。

請求項８

請求項５記載のポリシー設定支援ツールであって、

前記ポリシー設定支援ツールは、前記ポリシー情報に違反するアクセスが発生した場合に前記アクセス制御部から通知を受けて、当該アクセスの対象となるオブジェクトを管理するコンピュータシステムの利用者に対してメッセージを伝え、前記利用者による判断に基づいて所定の処理を実行する手段を備えており、

前記利用者による判断とは、前記ポリシー違反のアクセスを以後全て許可するか、今回のアクセスのみ許可するか、禁止するかのいずれかであり、

前記ポリシー違反のアクセスを以後全て許可する場合には、前記ポリシー設定支援ツールによる所定の処理として前記アクセスが正当なアクセスとなるようポリシー情報を変更し、前記アクセス制御部に対しては前記アクセスが正当であることを通知し、

前記ポリシー違反のアクセスを今回のみ許可する場合には、所定の処理として前記ポリシー情報は変更せずに、前記アクセス制御部に対しては前記アクセスが正当であることを通知し、

前記ポリシー違反のアクセスを禁止する場合には、所定の処理として前記ポリシー情報は変更せず、前記アクセス制御部に対しては前記アクセスが不正であることを通知する。

請求項９

請求項５記載のポリシー設定支援ツールであって、

前記ポリシー設定支援ツールは、前記ポリシー情報に登録されていないオブジェクトに対して、当該オブジェクトに関連付けられたサブジェクトからアクセスが発生した時に、前記アクセス制御部から通知を受け、前記コンピュータシステムの利用者に対してメッセージを伝え、前記利用者による判断に基づいて所定の処理を実行する手段を備えており、

前記利用者による判断とは、前記登録されていないオブジェクトに対する当該オブジェクトに関連付けられたサブジェクトからのアクセスを許可するか、禁止するかのいずれかであり、

前記アクセスを許可する場合には、前記ポリシー設定支援ツールによる所定の処理として前記アクセスが正当なアクセスとなるようポリシー情報を変更して、前記アクセス制御部に対しては前記アクセスが正当であることを通知し、

前記アクセスを禁止する場合には、前記ポリシー情報は変更せず、前記アクセス制御部に対しては前記アクセスが不正であることを通知する。

請求項１０

請求項５記載のポリシー設定支援ツールであって、

前記ポリシー設定支援ツールは、前記ポリシー情報に登録された情報とは一部異なるサ

ブジェクトからアクセスが発生した時に、前記アクセス制御部から通知を受け、前記コンピュータシステムの利用者に対してメッセージを伝え、前記利用者による判断に基づいて所定の処理を実行する手段を備えており、

前記利用者による判断とは、前記サブジェクトからのアクセスを許可するか、禁止するかのいずれかであり、

前記アクセスを許可する場合には、前記ポリシー設定支援ツールによる所定の処理として前記サブジェクトが正当なものとなるようポリシー情報を変更して、前記アクセス制御部に対しては前記アクセスが正当であることを通知し、

前記アクセスを禁止する場合には、前記ポリシー情報を変更せず、前記アクセス制御部に対しては前記アクセスが不正であることを通知する。

ABSTRACT

本発明が提供するポリシー設定支援ツールは、ソフトウェアの種類毎のポリシーを記述したサンプル情報と、オブジェクトの種類毎に利用頻度の高いプログラムの情報を記述した関連付け情報と、プログラムの動作を監視して記録したアクセスログ情報のいずれかを用いてポリシーの原案を作成するポリシー生成部１０２と、ポリシー原案を表示して、利用者による確認と編集を可能とするユーザインタフェース部１０１の処理により、適切なポリシー設定に必要な作業の簡易化を実現する。また差分検出部１０４により、設定済みポリシーから更新すべき部分を、現在のオブジェクト１１２とサブジェクト情報１１３を参照して検出し、ユーザインタフェース部１０１を通じて提示するとともに、簡易に更新可能とすることで、適切なポリシー維持も可能とする。